

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims:

1 Claim 1. (*Original*) A method for securing timestamping of digital data comprising the
2 steps of:
3 providing a secure encryption key; and,
4 providing a processor for performing security functions with the secure encryption key,
5 the processor operable in a first mode wherein the secure encryption key is used for encryption
6 operations and for test operations and in a second mode in which the secure encryption key is
7 only used for timestamping operations,
8 wherein once the processor performs a function with the secure encryption key in the
9 second mode, it is precluded from performing further functions in the first mode with the same
10 secure encryption key.

1 Claim 2. (*Original*) A method for securing timestamping of digital data as defined in
2 claim 1, comprising the steps of:
3 receiving a request to perform a timestamping operation; and,
4 placing the processor in the second mode of operation once the request is received.

1 Claim 3. (*Original*) A method for securing timestamping of digital data as defined in
2 claim 2, comprising the step of:
3 generating a unique code for being embedded within timestamped digital data, wherein
4 the secure encryption key and the processor are within a secure module and wherein the unique
5 code is indeterminable outside the secure module prior to receipt of the request.

1 Claim 4. (*Original*) A method for securing timestamping of digital data as defined in
2 claim 2, comprising the step of generating a unique code for being embedded within
3 timestamped digital data, the unique code being indeterminable before receipt of the request.

1 Claim 5. (*Original*) A method for securing timestamping of digital data as defined in
2 claim 4, wherein the unique code is inserted within each timestamped digital data.

1 Claim 6. (*Original*) A method for securing timestamping of digital data as defined in
2 claim 5, wherein each timestamped digital data comprises a timestamp, and wherein the unique
3 code is encoded within the timestamp.

Claim 7 (*Canceled*)

1 Claim 8. (*Previously Presented*) A method for securing timestamping of digital data as
2 defined in claim 3, wherein the unique code is generated based on the secure encryption key.

1 Claim 9. (*Previously Presented*) A method for securing timestamping of digital data as
2 defined in claim 3, wherein the unique code is generated based on a random number.

1 Claim 10. (*Previously Presented*) A method for securing timestamping of digital data as
2 defined in claim 3, wherein the unique code is generated based on a real time value indicative of
3 a time instance a first request has been received.

1 Claim 11. (*Original*) A method for securely timestamping digital data comprising the
2 steps of:

3 providing a secure encryption key;

4 providing a processor for performing security functions with the secure encryption key,
5 the processor operable in a first mode wherein the secure encryption key is used for encryption
6 operations and for test operations and in a second mode in which the secure encryption key is
7 only used for timestamping operations, wherein once the processor performs a function with the
8 secure encryption key in the second mode, it is precluded from performing further functions in
9 the first mode with the secure encryption key;

10 when the processor is in the first mode of operation, receiving a first request to perform a
11 timestamping operation on first digital data and then placing the processor in the second mode of
12 operation; and,

13 providing a unique code for being embedded within timestamped digital data, the unique
14 code being indeterminable before receipt of the first request.

1 Claim 12. (*Original*) A method for securely timestamping digital data as defined in
2 claim 11, comprising the steps of:

3 receiving from a real time clock data indicative of a real time the first request for a
4 timestamping operation has been received;

5 generating a first timestamp based on the data indicative of real time using the secure
6 encryption key;

7 embedding the first timestamp within the first digital data and inserting the unique code
8 within the first digital data; and,

9 encoding the first digital data with inserted data therein to form timestamped digital data.

1 Claim 13. (*Original*) A method for securely timestamping digital data as defined in
2 claim 12 wherein encoding includes the step of encrypting the digital data with the secure key.

1 Claim 14. (*Original*) A method for securely timestamping digital data as defined in
2 claim 13, comprising the steps of:

3 receiving a second request to perform a timestamping operation on second digital data;

4 receiving from the real time clock data indicative of a real time the second request for a
5 timestamping operation has been received;

6 generating a second timestamp based on the data indicative of a real time using the secure
7 encryption key;

8 embedding the second timestamp within the second digital data and inserting the unique
9 code within the second digital data; and,

10 encoding the second digital data with inserted data therein to form timestamped digital data.

1 Claim 15. (*Original*) A method for securely timestamping digital data comprising the
2 steps of:

3 providing a secure encryption key;

4 providing a processor for performing security functions with the secure encryption key,
5 the processor operable in a first mode wherein the secure encryption key is used for encryption
6 operations and for test operations and in a second mode in which the secure encryption key is
7 only used for timestamping operations, wherein once the processor performs a function with the
8 secure encryption key in the second mode, it is precluded from performing further functions with
9 the secure encryption key in the first mode;

10 placing the processor in the second mode of operation; and,

11 providing a unique code for being embedded within timestamped digital data, the unique
12 code being indeterminable before the processor is placed in the second mode of operation.

1 Claim 16. (*Original*) A method for securely timestamping digital data as defined in
2 claim 15, comprising the steps of:
3 receiving a request to perform a timestamping operation on digital data;
4 receiving from a real time clock data indicative of a real time value that the request for a
5 timestamping operation has been received;
6 generating a timestamp based on the data indicative of a real time using the secure
7 encryption key;
8 embedding the timestamp within the digital data;
9 inserting the unique code within the timestamped digital data; and,
10 encoding the digital data with the unique value and the timestamp embedded therein to
11 form timestamped digital data.

1 Claim 17. (*Original*) A method for securely timestamping digital data as defined in
2 claim 15, comprising the steps of:
3 receiving a request to perform a timestamping operation on digital data;
4 receiving from a real time clock data indicative of a real time the request for a
5 timestamping operation has been received;
6 hashing the digital data; and,
7 encrypting the hashed digital data with the data indicative of a real time using the secure
8 encryption key.

1 Claim 18. (*Original*) A method for securely timestamping digital data as defined in
2 claim 17, comprising the step of inserting the unique code within the hashed digital data prior to
3 encryption thereof.

Claim 19. (*Canceled*)

1 Claim 20. (*Previously Presented*) A secure system for securely timestamping digital data
2 comprising:

3 at least a first port for receiving the digital data and for providing timestamped digital
4 data; and

5 a processor for:

6 performing security functions with a secure encryption key, the processor operable in a
7 first mode wherein the secure encryption key is used for encryption operations and for test
8 operations and in a second mode in which the secure encryption key is only used for
9 timestamping operations, wherein once the processor performs a function with the secure
10 encryption key in the second mode, it is precluded from performing further functions with the
11 secure encryption key in the first mode.

1 Claim 21. (*Original*) A system for securely timestamping digital data as defined in
2 claim 20, comprising: a real time clock for providing data indicative of a real time.

1 Claim 22. (*Previously Presented*) A system for securely timestamping digital data as
2 defined in claim 21, wherein the processor comprises circuitry for generating the secure
3 encryption key.

1 Claim 23. (*Original*) A system for securely timestamping digital data as defined in
2 claim 22, wherein the processor comprises circuitry for generating a pseudo-random number
3 forming a unique value associated with an encryption key, the unique value for being embedded
4 within each timestamp formed with the associated key, the unique value being indeterminable
5 outside the system before the processor is placed in the second mode.

1 Claim 24. (*Original*) A system for securely timestamping digital data as defined in
2 claim 22, comprising secure memory for storing the secure encryption key inaccessible outside
3 of the secure system but accessible to the processor for performing security functions therewith,
4 wherein within the memory is stored a unique value associated with an encryption key, the
5 unique value for being embedded within each timestamp formed with the associated key, the
6 unique value being indeterminable outside the system before the processor is placed in the
7 second mode.

1 Claim 25. (*Original*) A system comprising:
2 a processor that processes a secure encryption key, said processor being operable in a
3 first mode that processes the secure encryption key in encryption operations, and in a second
4 mode that processes the secure encryption key in timestamping operations, wherein once the
5 processor processes the secure encryption key in the second mode, the processor is precluded
6 from processing the secure encryption key in the first mode.